



Управление
по
противодействию
киберпреступности
КМ УВД Брестского
облисполкома

Как не стать жертвой в киберпространстве

Основы безопасности



Динамика преступности в СВТ

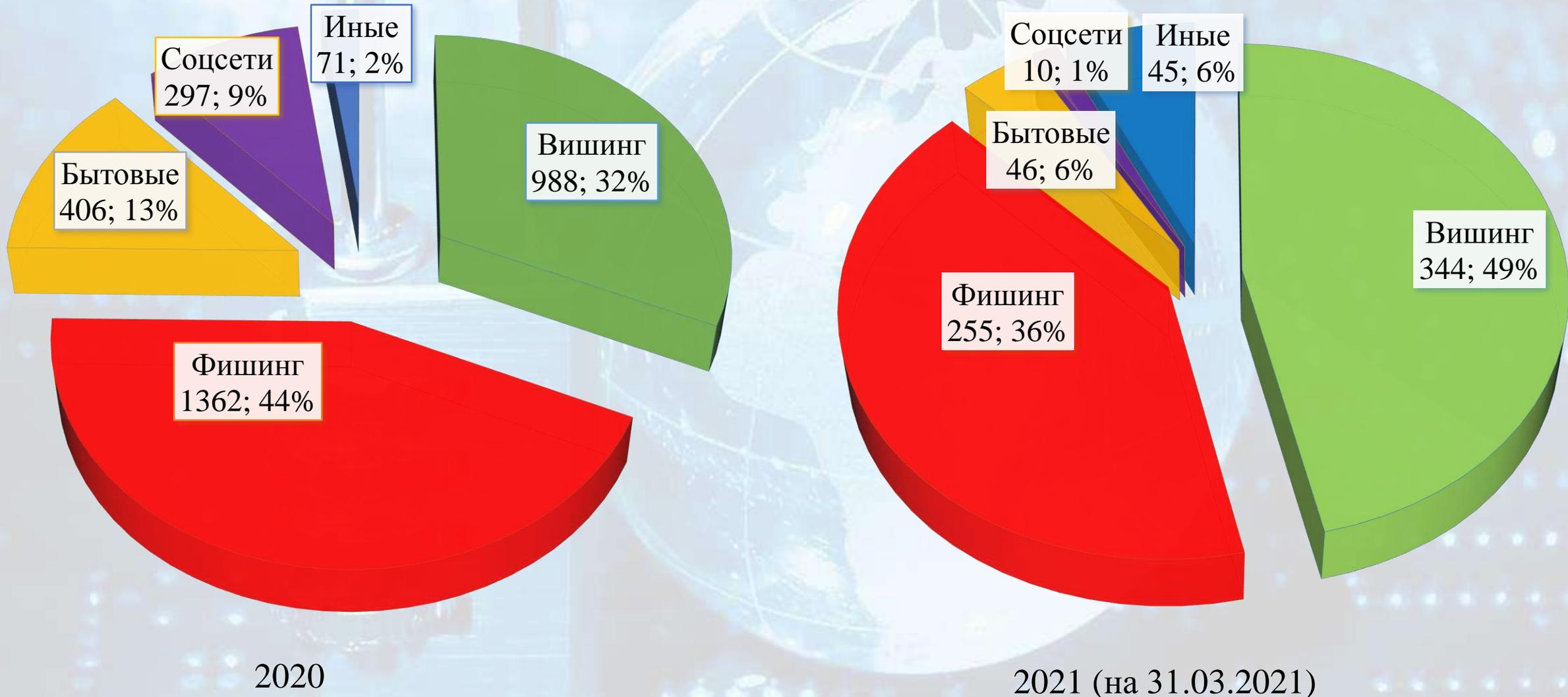
—●— Хищения

—●— Информационная безопасность





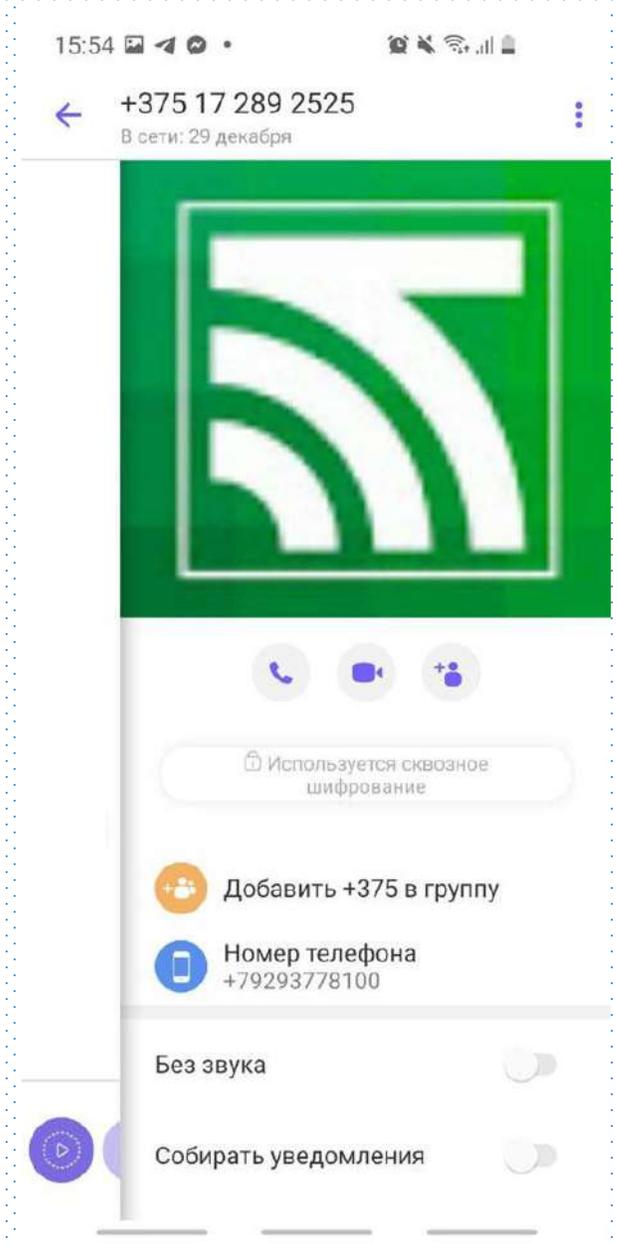
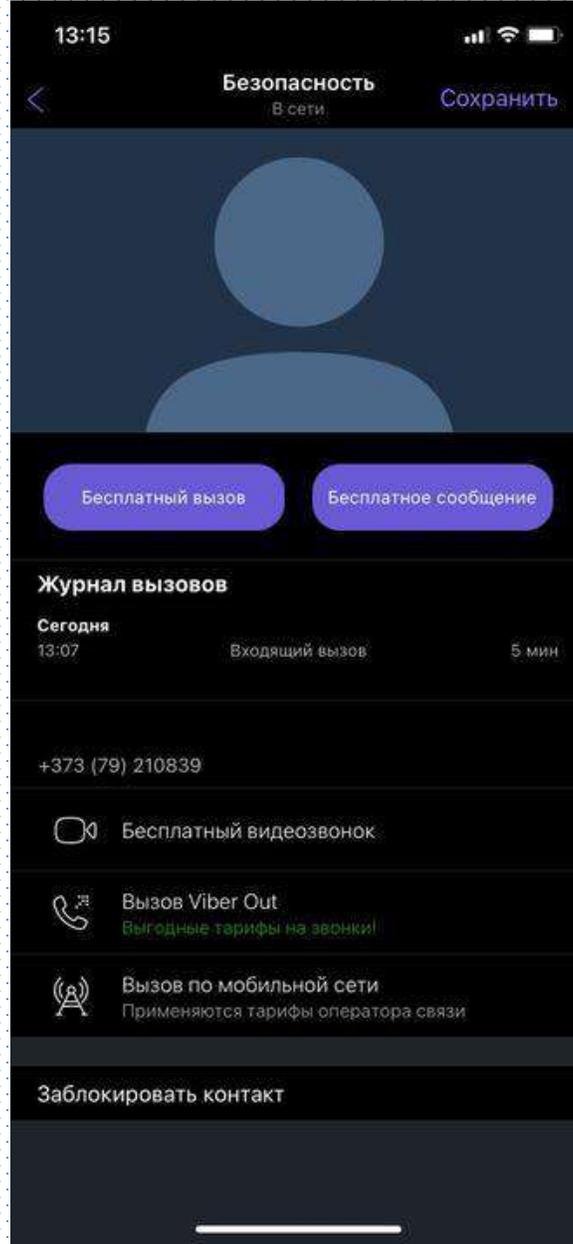
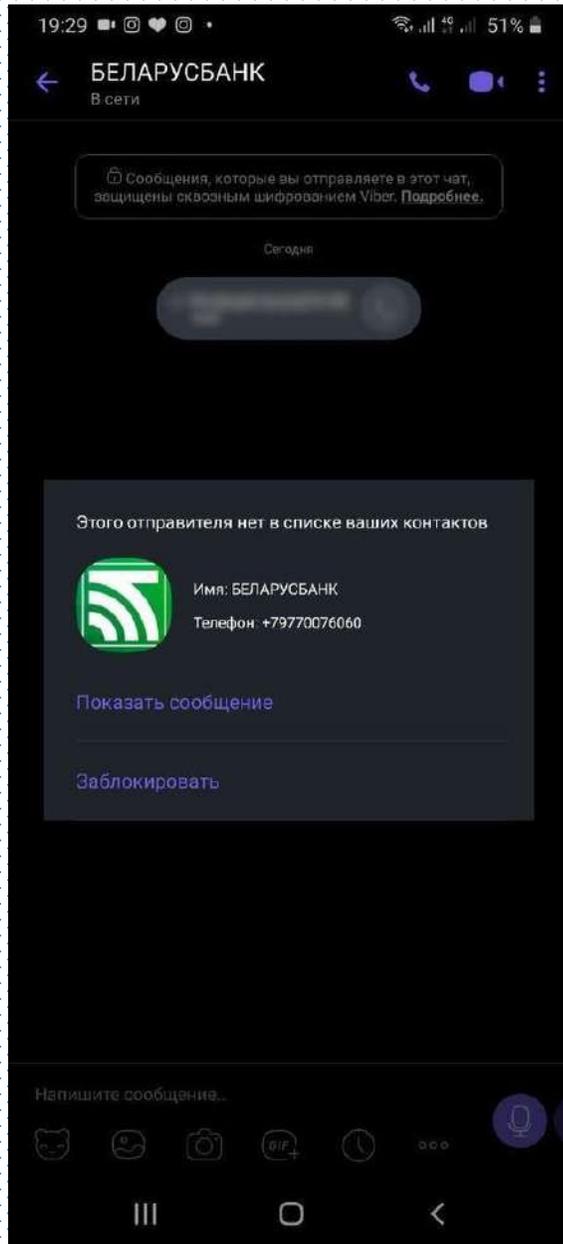
Структура высокотехнологичных преступлений (в разрезе 2020- первый квартал 2021г.)



Общее количество преступлений по линии СВТ - **3124**

Общее количество преступлений по линии СВТ - **708**

Примеры прозвонов «лжесотрудников» банковских учреждений



Если Вам поступил такой звонок



Следует помнить

- ни при каких обстоятельствах, никому и никогда не сообщайте информацию о себе или своей банковской платежной карте. Если Вам будет звонить настоящий сотрудник банка, то он точно будет знать, как минимум номер Вашей банковской платежной карты и никогда не спросит конфиденциальную информацию в телефонном режиме;
- уточните с кем именно Вы общаетесь, после чего положите трубку и перезвоните на номер телефона, который отображался у Вас на экране (в этом случае Вы свяжитесь именно с тем абонентом, которому принадлежит указанный номер, а не со злоумышленниками, которые его использовали с целью скрыть свой настоящий номер) и уточните суть возникшей проблемы;
- если же на Вас оказывается психологическое давление угрозами, что через несколько секунд Вы понесете финансовые потери, кто-то оформит на Вас кредит или что если Вы не сообщите требуемую информацию, то карту вообще заблокируют, не волнуйтесь, это обычная уловка преступников, главная цель которых ввести Вас в состояние неуверенности и страха потерять сбережения;
- сами перезвоните в свой банк или в круглосуточную службу сервиса, номер которой написан на оборотной стороне Вашей платежной карты и сообщите о случившемся.

!!!!Помните, если Вы сообщите злоумышленнику реквизиты своей банковской платежной карты, то он сможет распоряжаться всеми средствами на счету, а также оформить на Ваше имя дополнительные кредитные обязательства (онлайн-кредит)

Пример фишингового ресурса kufar24.space



kufar24.space Получение средств | ██████████

 **kufar**

Оформление и получение средств



300 р.
Шуба мутон новая

 **Ваш товар оформлен!**
Покупатель уже оплатил заказ.

Данные для отправления

Адрес доставки
ул. Молодежная ██████████

Фамилия	Имя	Отчество
Алексей	Владимирович	██████████

После получения средств на Вашу карту, пожалуйста отправьте товар покупателю по указанным данным, доступные пункты отправки товара можете посмотреть на официальном сайте [Белпочта](#)

После отправки товара укажите номер отправления покупателю! Товар следует отправить в течение 3-х суток с момента получения средств

 **БЕЛПОШТА** Доставка осуществляется через сервис Белпочта.

300 р.

[Получить средства](#)

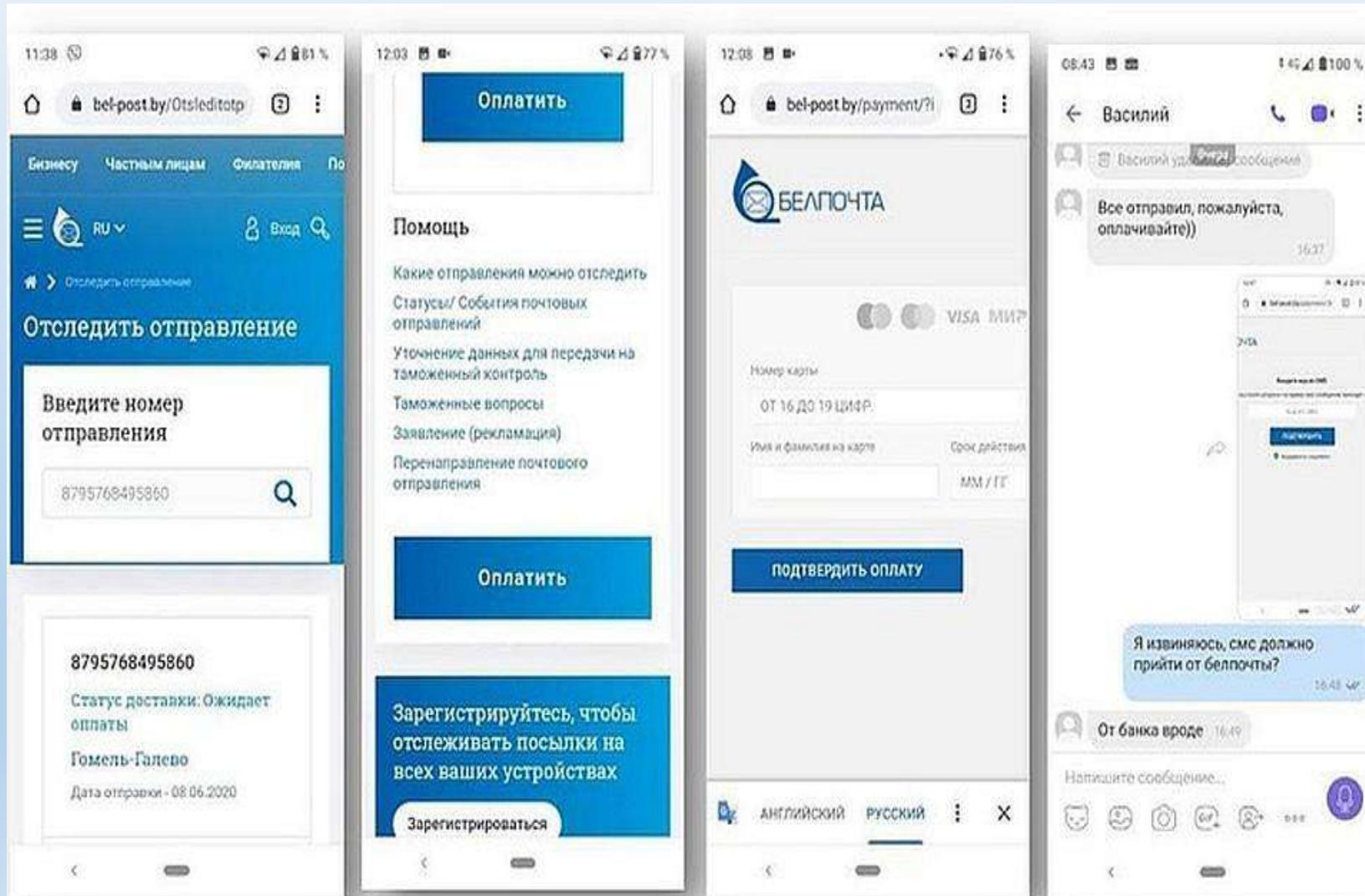
 **Проведение платежей безопасно!**

Нажимая кнопку «Получить средства», вы принимаете правила [Пользовательского соглашения](#) с использованием онлайн сервиса «Безопасная сделка»

ПОДДЕЛКА

CERT.BY

Пример «фишингового» ресурса bel-post.by





Как не стать жертвой киберпреступников, совершая сделки в сети Интернет

Следует помнить

- вести общение с потенциальными покупателями или продавцами только во внутреннем чате торговой площадки (зачастую торговые площадки блокируют возможность перехода на поддельные ресурсы);
- ведя общение с пользователем стоит перейти к его профилю и обратить внимание на дату создания (если он создан несколько дней назад, то это должно вызвать дополнительную настороженность);
- очень внимательно относиться к любому случаю, когда необходимо ввести данные карты или информацию, предоставленную банком (смс-код, логин или пароль от интернет-банкинга);
- уточнить у собеседника номер телефона если он не указан в объявлении, а потом позвоните на этот номер, чтобы убедиться, что он реален и принадлежит именно пользователю, с которым вы совершаете сделку;
- использовать отдельную банковскую карту для осуществления покупок в сети Интернет, на которой не хранятся денежные средства и на которую не поступает регулярный доход в виде заработной платы, стипендии или пенсии;
- избегать перехода по неизвестным интернет-ссылкам, которые предоставляются в ходе переписки якобы для получения предоплаты или оформления доставки.

!!!!Соблюдение этих несложных мер предосторожности позволит уберечь ваши денежные средства от преступных посягательств**!!!!**

Как не стать жертвой киберпреступника.

ЗАЩИТА БАНКОВСКОЙ КАРТОЧКИ



Основные правила информационной безопасности по защите банковской карточки:

-  хранить в тайне пин-код карты
-  прикрывать ладонью клавиатуру при вводе пин-кода
-  оформлять отдельную карту для онлайн-покупок
-  деньги зачислять только в размере предполагаемой покупки
-  использовать услугу 3-D Secure* и лимиты на максимальные суммы онлайн-операций
-  скрыть CVV-код на карте (трехзначный номер на обратной стороне), предварительно сохранив его
-  подключить услугу "SMS-оповещение"



Не рекомендуется

-  хранить пин-код вместе с карточкой/на карточке
-  сообщать CVV-код или отправлять его фото
-  распространять личные данные (например паспортные), логин и пароль доступа к системе "Интернет-банкинг"
-  сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли***, код авторизации, пароли 3-D Secure

* Услуга 3-D Secure - для подтверждения онлайн-платежа держатель карточки вводит особый код (получает его в смс-сообщении на телефон).

** Код CVV - последние 3 цифры номера на обратной стороне платежной карты справа на белой линии, предназначенной для подписи. Код дает возможность распоряжаться средствами, находящимися на счету, физически не контактируя с картой.

*** Сеансовый пароль - предоставляется при входе в интернет-банкинг, действителен лишь в течение одного платежного сеанса.



Источник: МВД Беларуси.

© Инфографика 



Как не стать жертвой киберпреступника

НАДЕЖНЫЕ ПАРОЛИ

01

НЕОБХОДИМО:

- + Создавать персональные (уникальные) пароли к разным сервисам и менять их каждые 3 месяца
- + Использовать сложные пароли: минимум 12 символов, одновременно цифры, строчные и прописные буквы, знаки пунктуации
- + Доверять только проверенным менеджерам паролей

НЕ РЕКОМЕНДУЕТСЯ:

- Использовать повторения символов
- Хранить пароли на бумажных носителях
- Использовать в качестве пароля свой логин (имя пользователя, учетная запись, никнейм)
- Сохранять пароль автоматически в браузере
- Использовать биографическую информацию в пароле

БЕЗОПАСНЫЙ WI-FI

02

НЕОБХОДИМО:

- + Отключить общий доступ к вашей Wi-Fi сети и использовать надежный пароль к ней
- + Обновить прошивку роутера и сменить пароль к административной панели
- + Запретить автоматическое подключение своих устройств к открытым Wi-Fi точкам

НЕ РЕКОМЕНДУЕТСЯ:

- Вводить свой логин и пароль доступа к учетной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговых центрах и т.д.

БРАУЗЕРЫ И САЙТЫ

03

НЕОБХОДИМО:

- + Обновлять браузер и плагины
- + Использовать VPN

НЕ РЕКОМЕНДУЕТСЯ:

- Переходить по непроверенным ссылкам
- Вводить информацию на сайтах, если соединение не защищено (нет https и )
- Сохранять персональные данные в браузере

ЗАЩИТА ОНЛАЙН-БАНКИНГА

04

НЕОБХОДИМО:

- + Хранить в тайне пин-код карты и другие банковские данные
- + Прикрывать ладонью клавиатуру при вводе пин-кода
- + Оформить отдельную карту для онлайн-покупок и не держать на ней большие суммы
- + Использовать лимиты на максимальные суммы онлайн-операций
- + Скрыть CVV-код на карте (трехзначный номер на обратной стороне), предварительно сохранив его

НЕ РЕКОМЕНДУЕТСЯ:

- Хранить пин-код вместе с карточкой/на карточке
- Сообщать CVV-код или отправлять его фото
- Распространять свои паспортные данные (информацию личного характера, номер мобильного телефона), логин и пароль для доступа к системе интернет-банкинга
- Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации и т.д.

ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕРОВ

05

НЕОБХОДИМО:

- + Устанавливать приложения только из официальных магазинов
- + Обращать внимание, к каким функциям устройства приложение запрашивает доступ
- + Обмениваться сообщениями в соцсетях и мессенджерах, только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения

НЕ РЕКОМЕНДУЕТСЯ:

- Размещать персональную и контактную информацию о себе в открытом доступе
- Указывать геолокацию на фото в постах
- Отвечать на обидные выражения и агрессию в соцсетях – лучше напишите об этом администратору ресурса
- Употреблять ненормативную лексику при общении
- Устанавливать приложения с низким рейтингом и негативными отзывами

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ

06

НЕОБХОДИМО:

- + Подключить двухфакторную аутентификацию
- + Использовать разную почту для переписок и для регистраций на сайтах
- + Использовать спам-фильтры

НЕ РЕКОМЕНДУЕТСЯ:

- Реагировать на письма от неизвестного отправителя – скорее всего это спам или мошенники
- Открывать подозрительное вложение к письму – сначала позвоните отправителю и узнайте, что это за файл

Типичные действия злоумышленника после несанкционированного доступа к чужим аккаунтам



- ❖ рассылка всем виртуальным «друзьям» потерпевшего просьбы под различными предложениями сообщить реквизиты банковской платежной карты. Это может быть ее фото или просто номер, срок действия и иные реквизиты;
- ❖ изучение содержания переписок потерпевшего и использование их содержания в качестве инструмента для вымогательства денежных средств (личные диалоги на откровенные темы, фотографии, содержащиеся на странице и в диалогах и иные очень личные данные);
- ❖ Рассылка различного рода порочащей информации от имени владельца страницы иным пользователям, ссылок на поддельные ресурсы банковских учреждений, а также вредоносное программное обеспечение

!!!! В случае обнаружения «взлома» аккаунта, прежде всего следует попытаться восстановить доступ к нему путем отправки сообщения на «привязанный» номер мобильного телефона или электронную почту, оповестить друзей и знакомых об инциденте, используя при этом иные соцсети и мессенджеры **!!!!**





Преступления против информационной безопасности:

- ст.349 УК РБ. Несанкционированный доступ к компьютерной информации
- ст.350 УК РБ. Модификация компьютерной информации
- ст.351 УК РБ. Компьютерный саботаж
- ст.352 УК РБ. Неправомерное завладение компьютерной информацией
- ст.353 УК РБ. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе
- ст.354 УК РБ. Разработка, использование либо распространение вредоносных программ
- ст.355 УК РБ. Нарушение правил эксплуатации компьютерной системы или сети

Правила информационной безопасности:

- ◆ Не устанавливать программное обеспечение из неизвестных источников
- ◆ Не открывать электронных писем от неизвестных отправителей, не переходить по ссылкам и не запускать вложенные файлы
- ◆ Использовать наиболее современную версию антивирусного программного обеспечения
- ◆ Использовать безопасные (сложные пароли), а также механизмы дополнительной аутентификации
- ◆ Хранить пароли в тайне от близких
- ◆ Не осуществлять переходов по подозрительным ссылкам и не вводить личную информацию (номера карт, телефонов и т.п.)